Turvaintsidendid

- praktiline intsidendi haldus
- andmete analüüs (arvutikriminalistika)

Peeter Tatter

Turvaintsidendid

- On saabunud olukord, kus:
  - miski ei tööta või teeb midagi valesti
  - midagi on puudu
  - midagi on üle (nt logifailides)
  - …

Esimesed sammud peale intsidendi teadvustamist

- Esmane hinnang – millega on tegemist
- Organisatsioonilised küsimused
  - Kes on pädev otsustama edasist tegevust?
  - Kas tekkinud situatsiooni jaoks on olemas mingi tegevuskava või plaan?
  - Keda intsident veel puudutab ning keda kaasata olukorra lahendamisesse?
- Kas tegu võib olla situatsiooniga, mis viib lõpuks kriminaalmenetluseni?

Esmase info analüüs

- Olulised esimesed küsimused:
  - millal, kes ja mida märkas?
  - mida on juba ette võetud ning milliste tulemustega?
  - kuidas saada täpsemalt teada, mis toimus?
  - kuidas edasi toimida?
  - info haldamine

Süsteemi kiire taastamine vs andmete säilitamine

- Kuidas süsteem/teenus kiiresti taastada?
  - laseme käima varusüsteemi, katkise jätame analüüsimiseks
  - taastame süsteemi puhtale andmekandjale, katkise süsteemiga andmekandja jätame analüüsimiseks
  - torgime vana süsteemi kuidagi käima, küll pärast analüüsime

Valikuid on…

Andmete kogumine - allikad

- Arvutid ise
- Erinevad logid
  - serverid
  - tulemüürid
  - juurdepääsu- ja valvesüsteemid
- Turvakaamerate salvestused
- Asjaga kokkupuutunud inimesed
- Varukoopiad

Kogutud andmete säilitamine ning edastamine

- Arvutite puhul võimalikud erinevad variandid:
  - säilitada terve arvuti
  - Säilitada arvutis olnud andmekandja
  - teha andmekandjal olevatest andmetest tõmmis
  - kopeerida andmekandjalt välja olulised failid
- Logifailid
  - mitte liiga palju filtreerida
  - soovitavalt kontrollsummad

Arvutis olevate andmete analüüs

Kus on andmed – andmekandjatel muidugi

Põhireegel: igati tuleb vältida andmekandjatel asunud andmete muutmist

Traditsiooniline lähenemine uuritavale arvutile:

- mittetöötavat arvutit mitte käivitada
- töötavat arvutit mitte torkida, eemaldada toide (sülearvutil toide ja aku)
- fikseerida arvutiga ühendatud välised seadmed ja ühendused
- juhtmed lahti, arvuti kaasa ja rahulikult analüüsima…

Esimesed sammud uuritava masinaga

Kast on Teie laual

- Millest alustada?

Arvutianalüüsi põhitõed

Originaalset süsteemi kasutatakse nii vähe kui võimalik

- operatsioonisüsteemi käivitamine originaalselt andmekandjalt – mitte kunagi
- andmekandjad eraldatakse arvutist ning kopeeritakse nendel asuvad andmed
- teatud juhtudel on aktsepteeritav originaalse arvuti käivitamine spetsiaalse boot-CD või -disketiga

Põhimõte: saada andmed turvalisse kohta ära ning kasutada analüüsimiseks kindlaid vahendeid

Andmete kopeerimine analüüsiks I

Eelistatud meetodid:

- kettalt-kettale (*cloning*)
- kettalt-faili (*disk imaging*)

teatud juhtudel aktsepteeritavad:

- kettajaotiselt-faili (*volume imaging*)
- failisüsteemist-faili (*logical imaging*)
- failisüsteemist-failisüsteemi (*copying*)

Andmete kopeerimine analüüsiks II

Võimalused kopeeritud andmete autentsuse ning terviklikkuse kontrolliks

- originaali ja klooni või tõmmise kontrollsummad (MD5/SHA1)
- tõmmise väiksemate plokkide kaupa (CRC)
- kontrollsummad failide kaupa

Andmete kopeerimine analüüsiks III

Tõmmiste formaadid

- dd (*raw image*)
  - kõige universaalsem
  - puuduvad spetsiaalsed vahendid tõmmise terviklikkuse kontrolliks
- E0x
  - hetkel *de facto* standard (EnCase)
  - sisaldab kopeerimisel arvutatud kontrollsummasid (MD5, CRC)
  - sisaldab tõmmist iseloomustavat metainfot
  - suletud formaat

Andmete kopeerimine analüüsiks IV

Kaalutlused kopeerimisel kasutatava süsteemi valikul:

- MS-DOS
- Linux
- Live CD-d (Helix)
- Windows???

- midagi spetsiaalset

Andmete kopeerimine analüüsiks V

Abivahendid - nn “riistvaraline kirjutuskaitse” (*write blocker*)

- kirjutusoperatsioonid andmekandjale on blokeeritud ketta liidese tasemel
- ei esita mingeid täiendavaid nõudeid arvuti riist- ja tarkvarale
- lubavad analüüsitavate andmekandjate kuumvahetamist (*hot-swap*)
- arvutipoolne liides: SCSI, PATA, USB2, FireWire-400 (IEEE1394), FireWire-800 (IEEE1394B), eSATA
- andmekandjapoolne liides: SCSI, PATA, SATA

Andmete kopeerimine analüüsiks VI

Tarkvara:

- dd
- sdd, ddrescue, dd_rescue, dcfldd, rdd, dc3dd
- en.exe, linen (EnCase)

- FTK Imager (FTK)
- EnCase

- Norton Ghost ja teised üldotstarbelised kloonimisvahendid???

Andmete kopeerimine analüüsiks VII

Riistvara – kloonimisseadmed (*forensic disc duplicators*):

- kaasaskantav iseseisev seade
- võimaldavad nii kloonimist kui tõmmiseid
- kiirused kuni 4GB/min
- kontrollsumma arvutamine kopeerimise käigus
- automaatne tegevuste logimine

Enamlevinud sedmed:

- Logicube MD5/Talon/Quest
- Tableau TD1
- ImageMASSter Solo

Peale kopeerimist, enne analüüsi

Andmed kopeeritud, mis edasi?

- Kontrollime kohe klooni/tõmmise autentsust ja terviklikkust
- Fikseerime arvuti kellaaja/kuupäeva
- Teeme kopeeritud andmetest (kloonist või tõmmisest) varukoopia

Aeg hakata mõtlema analüüsivahenditele…

Analüüsivahendid - võimalused

- Erinevate failisüsteemide interpreteerimine
  - FAT12, FAT16, FAT32
  - NTFS
  - EXT2/EXT3, Reiser
  - HFS/HFS+
  - FFS/UFS/UFS2
  - ISO9660/Joliet/UDF

Analüüsivahendid - võimalused

- Kustutatud failide “taastamine”:
  - andmed on tõeliselt kustutatud alles siis kui andmete salvestamiseks kasutatud baidid on uute andmetega üle kirjutatud
  - failisüsteemis kustutatuks märgitud failikirjete interpreteerimine
  - kustutatud kataloogikirjete otsing
  - imesid paraku ei tee, ülekirjutatud infot ei taasta

Analüüsivahendid - võimalused

- Failide poolt hõivamata ruum
  - failisüsteemi hetkel kasutamata klastrid
  - faili füüsiline ja loogiline suurus, faili šlakk (*file slack*)
  - kettajaotiste poolt hõivamata ruum

See ruum võib olla äärest ääreni täis andmeid kunagi eksisteerinud failidest – kuidas seda infot leida?

Analüüsivahendid - võimalused

Märksõnaotsingud

- reaalajas otsing
- indekseerimine/otsing indeksist
- regexp-otsing

erinevad kodeeringud

erinevad otsingustrateegiad

Analüüsivahendid - võimalused

- failide sisu interpreteerimine (eelvaade)
- pildigalerii
- failide signatuuride kontroll, vastavus laiendiga
- failide kontrollsummade võrdlemine mingi eelnevalt defineeritud kontrollsummadega
- oluliste andmete märgistamine, järjehoidjad
- (pool)automaatne dokumenteerimine, kokkuvõtted, protokollid

Analüüsivahendid

Ajalooliselt esimesed:

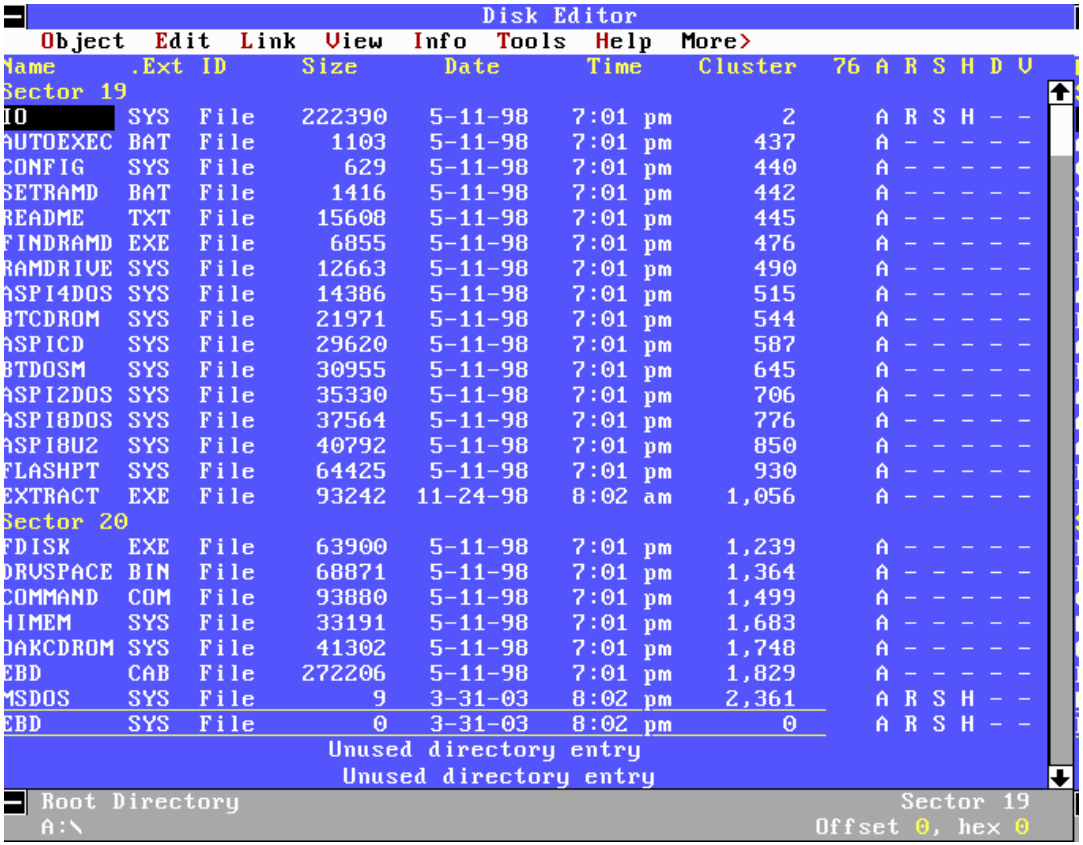
- Norton Disk Edit (diskedit.exe)
- TCT - The Coroners Toolkit

Praegu aktuaalsed:

- TSK (The Sleuth Kit)
  - Autopsy
  - PTK
- EnCase
- FTK (Forensic Toolkit)
- X-Ways Forensics (WinHex)

Analüüsivahendid – Norton Disk Edit

- üks esimesi tööks kasutatud vahendeid
- ei ole spetsiaaltarkvara
- oskab interpreteerida vaid FAT-failisüsteeme
- kasutusel tänapäeval enamasti õppevahendina
- olemas palju edasi-arendusi



Analüüsivahendid - TCT

The Coroners Toolkit

- esitletud 1991,
  D. Farmer ja W. Vienema
- peaasjalikult mõeldud Unixiliste analüüsiks
- kollektsioon käsurea vahendeid, Perl ja C
- tasuta tarkvara
  (IBM Public Licence)

René Magritte "La trahison des images"

http://www.porcupine.org/forensics/tct.html

Analüüsivahendid - TSK

The Sleuth Kit

- kogum käsurea vahendeid
- TCT edasiarendus
- töötab Linux, OS X, FreeBSD, OpenBSD, and Solaris süsteemides
- tunneb FAT, NTFS, UFS, EXT2FS, and EXT3FS failisüsteeme
- tasuta tarkvara (CPL, IBM Public License)

http://www.sleuthkit.org/sleuthkit/

Analüüsivahendid – Autopsy ja PTK

mõlemad on graafilised kasutajaliidesed, mis kasutavad TSK vahendeid

- Autopsy – originaalne TSK tiimi poolt loodud liides
- PTK – DFLabs'i poolt loodud alternatiivne liides

http://www.sleuthkit.org/autopsy/
http://ptk.dflabs.com/

Analüüsivahendid - EnCase

- MS Windowsi platvormil analüüsikeskkond
- Hetkel väga levinud, *de facto* standard
- intuitiivne ning kasutajasõbralik kõik-koos liides
- erinevad versioonid erinevateks ülesanneteks, moodulid vähemvajalike omaduste realiseerimiseks
- väga hea kasutajatugi, toimiv ja omavahel suhtlev kasutajate kogukond
- kinnine kommertstarkvara, suhteliselt kallis

Analüüsivahendid - FTK

- MS Windowsi platvormil analüüsikeskkond
- teine hetke enimkasutatavates vahenditest
- kasutajasõbralik ning vähem tehniline kui EnCase, parem ülevaade – kuid vähem võimalusi
- võimas eelnevat indekseerimist toetav otsingumootor
- toetab vähe failisüsteeme
- areng on olnud aeglane ning takerduv
- kinnine kommertstarkvara

Analüüsivahendid – võrdlus

- käsureavahendite puhul saab suure *case*'i puhul probleemiks asjast ülevaate saamine/säilitamine, töö nõuab ranget metoodilisust ning dokumenteerimist
- käsureavahendite (ning nendel põhinevate brauseri-põhiste liideste) puhul on raske säilitada "turvalise liivakasti" põhimõtet
- GUI-ga vahendite puhul võib väga kergelt jäädagi ainult "ringi surfama", vahendite intuitiivsus võib olla petlik
- paremate asjade eest küsitakse piinlikult palju raha
- ükski asi ei tee päris kõike

Traditsiooniline arvutikriminalistika vs “*live forensics*”

- Traditsiooniline arvutikriminalistika
  - esmatähtis andmekandjatel olevate andmete muutmise vältimine
- “live forensics”
  - esmatähtis andmekandjatel olevate andmete minimaalne muutmine, talletades ka operatiivmälus olevad andmed

Töötava arvuti analüüs I

Täiendavad andmed töötavast arvutist:

- hetkel aktiivsed protsessid ja nende andmed
- hetkel aktiivsed võrguühendused
- monteeritud krüptokettad või –konteinerid
- muu operatiivmälus sisalduv info

Kuidas talletada kõik see, säilitades maksimaalselt muutmatuna ka andmekandjatel olevad andmed?

Töötava arvuti analüüs II

Kuidas analüüsida töötavat arvutit – käsitsi?

- fikseerida töötavad programmid, aktiivsed protsessid, aktiivsed võrguühendused
- fikseerida arvutis ilmselt nähtavad andmekandjad, vajadusel teha neil asuvatest andmetest tõmmis
- …
- toide tagant ning kettaid analüüsima…

Ka variant, kui muid vahendeid käepärast ei ole…

Töötava arvuti analüüs III

Olemas hulk eraldi vahendeid mälus olevate andmete kuvamiseks või talletamiseks:

- psinfo/pslist/psfile/psloggedon (SysInternals)
- PMDump/MemImager (Arne Vidstrom)
- mdd (SourceForge)
- winen (EnCase paketis)

Töötava arvuti analüüs IV

Samuti olemas valmis paketid töö automatiseerimiseks:

- WFT (Windows Forensic Toolchest)
- COFEE (Computer Online Forensic Evidence Extractor)